REMARKS

The present Amendment amends claims 17-19, leaves claims 20-24 unchanged and cancels claim 16. Therefore, the present application has pending claims 17-24.

In paragraph 1 of the Office Action the Examiner objected to claim 17 as containing an informality, namely a typographical error. An amendment was made to claim 17 to correct the informality noted by the Examiner. Therefore, this objection is overcome and should be withdrawn.

Claims 16-19 stand rejected under 35 USC §102(b) as being anticipated by Takagi (U.S. Patent No. 5,109,152). As indicated above, claim 16 was canceled. Therefore, this rejection with respect to claim 16 is rendered moot. This rejection with respect to claims 17-19 is traversed for the following reasons. Applicants submit that the features of the present invention as now recited in claims 17-19 are not taught or suggested by Takagi whether taken individually or in combination with any of the other references of record. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Amendments were made to each of claims 17-19 so as to more clearly recite that the present invention is directed to a method, computer program and authentication system for performing authentication between a client and a service server connected over a network. According to the present invention, a client generates a random number, ciphers the random number and transmits the random number thus ciphered to the service server. The service server deciphers the ciphered random number transmitted from the client, reciphers the random thus

deciphered and transmits the random number thus reciphered to the client. The client thereafter re-deciphers the reciphered random number, confirms whether the random number thus re-deciphered coincides with the random number generated by the client and sends an inquiry about start of a service to the service server based on a result of the confirmation about the random number.

According to the present invention, when reciphering the deciphered random number, the service server not only reciphers the deciphered random number but also ciphers a code indicating the service server and transmits the reciphered random number and the code thus ciphered to the client. In addition, according to the present invention, when the reciphered random number is deciphered the client not only redeciphers the reciphered random number but also deciphers the ciphered code, confirms whether a service server which transmitted the reciphered random number and the ciphered code coincides with the service server to which the client transmitted the ciphered random number and sends the inquiry about start of the service to the service server based on a result of the confirmation about the service server.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record whether taken individually or in combination with each other. Particularly, the above described features of the present invention now more clearly recited in the claims are not taught or suggested by Takagi.

Takagi teaches authentication of an IC card in communications between the IC card and an IC card terminal. Takagi specifically discloses the following steps as illustrated in Fig. 1 thereof including:

(1) An IC card (10 in FIG. 1) generates a random number (11), ciphers (12) the random number with a ciphering key 1 (KE1) stored in advance, and transmits the random number thus ciphered to a card terminal;

(2) The card terminal (20) deciphers the ciphered random number with a deciphering key 1 (KD1) stored in advance, and identifies (21) the random number;

(3) The card terminal ciphers the random number with a ciphering key 2 (KE2) stored in advance, and returns the random number thus ciphered to the IC card;

(4) The IC card deciphers the ciphered random number with a deciphering key 2 (KD2), and identifies (13) the random number; and

(5) The IC card compares (16) the random number generated at Step (1) and the random number identified at Step (4). If matched, the IC card prepares (17) transmission data, and starts (14) communication by ciphering the transmission data with the random number.

Thus, as is clear from the above the features of Takagi et al reside in that a random number ciphered with predetermined ciphering keys comes and goes in advance between the IC card and the card terminal, thereby enabling confirmation of partners and an exchange of ciphered data.

In contrast, the present invention as recited in the claims is directed not only to the confirmation of partners by utilizing matching by means of ciphering and deciphering keys, but also to features wherein a client actually receives information

specifying a server, namely a code indicating a service server, by which the client can specify a partner as a communication destination. These features are not taught or suggested by Takagi.

Therefore, Takagi fails to teach or suggest that when reciphering the reciphered random number, the client not only deciphers the reciphered random number but also deciphers the ciphered code, confirms whether a service server which transmitted the reciphered random number and the ciphered code coincides with the service server to which the client transmitted the ciphered random number, and sends the inquiry about start of the service to the service server, based on result of the confirmation about the service server as recited in the claims.

In the Office Action, the Examiner alleges that the Takagi's transmission data" corresponds to the applicant's "code indicating said service server". It is apparent, however, from the description of FIG. 1 in Takagi et al for example that Takagi's "transmission data" is data itself to be sent from the IC card to the card terminal, not "data indicating a service server" (i.e., data indicating a card terminal) as in the present invention.

In fact, Takagi an IC card user goes to the IC card terminal. Thus, in Takagi the IC card user knows apparently who is a partner of communication. Therefore, such data as the applicant's "code indicating said service server" is not needed in the Takagi's system, though confirmation of a communication partner may be needed.

Thus, the features of the present invention or recited in the claims are not taught or suggested by Takagi. Therefore, based on the above, Applicants

respectfully request the Examiner to reconsider and withdraw the 35 USC §102(b) rejection of claims 17-19 as being anticipated by Takagi.

Claims 20-24 stand rejected under 35 USC §102(b) as being anticipated by Leith (U.S. Patent No. 5,196,840). This rejection is traversed for the following reasons. Applicants submit that the features of the present invention as recited in claims 20-24 are not taught or suggested by Leith whether taken individually or in combination with any of the other references of record. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

The features of the present invention as recited in claims 20-24 are not taught or suggested by Leith whether taken individually or in combination with any of the other references of record.

Leith teaches prevention of faking by a third party who acquired information transmitted over networks in communications between computers via networks. Leith discloses the following steps in FIGS. 3-4, thereof as indicated by the Examiner:

(1) A user requesting an access transmits a user ID to a host as an access destination;

(2) The access destination host identifies a PIN (Personal identification Number) corresponding to the user ID by using own DB previously managed by the host;

(3) The access destination host generates a random number, ciphers the PIN with the random number, and returns the ciphered PIN to the user;

(4) The user deciphers the ciphered PIN by using the PIN managed by the user himself/herself, and identifies the random number;

(5) The user ciphers the PIN managed by the user himself/herself with the random number thus identified, and transmits the ciphered PIN to the access destination host; and

(6) The access destination host deciphers the ciphered PIN by using the random number already generated, identifies the PIN, compares the PIN identified at this step and the PIN identified at Step (2), and determines validity of communication.

Namely, the features of Leith is directed to preventing a PIN from being transmitted as plain text.

In contrast, the present invention as recited in the claims, not only the second computer to be accessed (corresponding to the access destination host) can identify a communication partner, but also the first computer (corresponding to the user) on the accessing side (or the communication starting side) can identify a communication partner. In other words, according to the present invention the computer to be accessed can identify the accessing computer by means of "a certificate being attached to said service request" as, for example, recited in claim 20. Further, according to the present invention, the accessing computer can identify the computer to be accessed by means of "a code indicating said second computer". These features of the present invention are clearly not taught or suggested by Leith.

Therefore, Leith fails to teach or suggest deciphering, by the second computer, the ciphered random number reciphering the random number thus deciphered and ciphering a code indicating the second computer both using a private code of the second computer, and transmitting the random thus reciphered and the code thus ciphered to the first computer as recited in the claims.

In the Office Action, the Examiner alleges that the Leith's "PIN" corresponds to the applicant's "code indicating said second computer". It is apparent, however, that Leith's "PIN" is not information identifying an access destination host, because Leith's "PIN" is information as to the accessing side (i.e., the user). In fact, Leith et al teaches how to hide "PIN" in communications. Thus, the "code indicating said service server" as recited in the claims is not needed in the Leith's system.

Thus, the features of the present invention as recited in the claims are not taught or suggested by Leith. Therefore, based on the above, Applicants respectfully request the Examiner to reconsider and withdraw the 35 USC §102(b) rejection of the claims as being anticipated by Leith.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 16-24.

In view of the foregoing amendments and remarks, Applicants submit that claims 17-24 are in condition for allowance. Accordingly, early allowance of claims 17-24 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (500.36158CX1).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 312-6600